108TH CONGRESS } HOUSE OF REPRESENTATIVES { REPORT
1st Session } { 108–305

GOVERNMENT NETWORK SECURITY ACT OF 2003

OCTOBER 7, 2003.—Committed to the Committee of the Whole House on the State of the Union and order to be printed

Mr. TOM DAVIS of Virginia, from the Committee on Government Reform, submitted the following

R E P O R T

[To accompany H.R. 3159]

[Including cost estimate of the Congressional Budget Office]

The Committee on Government Reform, to whom was referred the bill (H.R. 3159) to require Federal agencies to develop and implement plans to protect the security and privacy of government computer systems from the risks posed by peer-to-peer file sharing, having considered the same, report favorably thereon without amendment and recommend that the bill do pass.

CONTENTS

COMMITTEE STATEMENT AND VIEWS

Purpose

H.R. 3159 requires that federal agencies address the security and privacy risks posed by peer-to-peer file sharing programs when developing their network policies and procedures. Agencies must ensure that federal computers and the important information they

store remain secure, private, and protected, but agencies are given the flexibility to develop the most appropriate means of accomplishing this goal through a combination of technological means (such as firewalls) or non-technological means (such as employee training).

Background and need for the legislation

Peer-to-peer file-sharing programs are Internet applications that allow computer users to share electronic files with other users connected to a common file sharing network. Peer-to-peer file sharing programs can be used to share any type of electronic files, but are commonly used to share music, movies, and video games.

Peer-to-peer file sharing programs have become increasingly popular in recent years. One such program, Kazaa, has been downloaded nearly 280 million times—more than any other software program in Internet history. Other popular programs include BearShare and iMesh.

Peer-to-peer file-sharing programs increase the connectivity between computers connected to a common peer-to-peer network. This heightened connectivity can expose computers to risks beyond those raised by other Internet activities.

A user of a peer-to-peer file sharing program chooses which folders on his or her computer are available for sharing with others on the same peer-to-peer network. Because peer-to-peer file-sharing programs allow the sharing of any type of electronic data, every computer file in these shared folders becomes accessible to every other user on the peer-to-peer network. A peer-to-peer user who chooses to share a folder containing a music collection may not be aware that he or she is also sharing every personal document that might be stored in the same location.

A recent Government Reform Committee investigation found that peer-to-peer users are sharing more than movies, music, and video games. Using a search tool built into the Kazaa program, staff investigators found users sharing completed tax forms, medical records, and complete e-mail inboxes.

This increased connectivity of peer-to-peer file sharing also means that the computers used to operate these programs can be at greater risk for viruses and other malicious files. At a May 2003 Government Reform Committee hearing, leading network security experts testified on how viruses and worms can multiply on these peer-to-peer networks and enter into a user's computer through a peer-to-peer file sharing program.

The security risks of peer-to-peer file sharing programs potentially become far more serious when federal government computers are used to connect to peer-to-peer networks. The electronic information exposed may include data vital to national security and personal files about citizens such as financial, military, and medical records. Additionally, peer-to-peer use on even one computer can introduce viruses and worms to critical government networks, potentially slowing the functioning of the affected agency.

The United States House of Representatives and Senate recognized the risks of peer-to-peer file sharing nearly two years ago. The House and Senate are successfully protecting the privacy and security of congressional computers from the risks of peer-to-peer

file sharing through firewall technologies and employee policies on appropriate computer use.

Although Congress has addressed the risks of peer-to-peer file sharing, many federal government agencies have not taken the steps necessary to protect their networks and computers. A General Accounting Office investigation requested by the Government Reform Committee has found computers actively using peer-to-peer file sharing at federal agencies entrusted with sensitive government information, including a Department of Energy nuclear laboratory and a facility that manages NASA's space flight research.

Committee actions

H.R. 3159 was introduced by the Committee on Government Reform's Ranking Minority Member, Henry Waxman (CA), and the Committee's Chairman, Tom Davis (VA), on September 24, 2003. It is cosponsored by several members of the Government Reform Committee, including Rep. Christopher Shays (CT), Rep. John McHugh (NY), Rep. Wm. Lacy Clay (MO), Rep. Edolphus Towns (NY), Rep. John Carter (TX), Rep. Christopher Van Hollen (MD), Rep. Ileana Ros-Lehtinen (FL), Rep. Chris Bell (TX), Rep. Mark Souder (IN), Rep. Candice Miller (MI), Rep. Dan Burton (IN), Rep. Ed Schrock (VA), Rep. Stephen Lynch (MA), Rep. Dutch Ruppersberger (MD), Rep. Adam Putnam (FL), Rep. Elijah Cummings (MD), Rep. Linda Sanchez (CA), Rep. Tom Lantos (CA), Rep. Carolyn Maloney (NY), Rep. Major Owens (NY), Rep. Dianne Watson (CA), Rep. Doug Ose (CA), Rep. Jim Cooper (TN), Del. Eleanor Holmes Norton (DC), Rep. Danny Davis (IL), Rep. Joanne Davis (VA), Rep. Mike Turner (OH), and Rep. Todd Platts (PA). The bill was referred to the Committee on Government Reform.

On September 25, 2003, the Committee on Government Reform met in open session to consider H.R. 3159 along with four other measures. The committee favorably approved the bill by voice vote and reported it to the House of Representatives.

Committee hearings and testimony

On May 15, 2003, the Committee on Government Reform held a hearing entitled "The Threats to Privacy and Security on File Sharing Networks."[1] The purpose of the hearing was for the Committee to assess the security and privacy risks posed by the use of peer-to-peer file sharing programs. Witnesses at the hearing included Nathaniel S. Good, School of Information Management Systems, University of California, Berkeley; Jeffrey I. Schiller, Network Manager and Security Architect, Massachusetts Institute of Technology; Dr. John Hale, Assistant Professor of Computer Science and Director, Center for Information Security, the University of Tulsa; and James E. Farnan, Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation. These computer security experts expressed significant concern about security vulnerabilities associated with peer-to-peer file-sharing programs. Other witnesses included Alan B. Davidson, Associate Director, Center for Democracy and Technology; Derek S. Broes, Executive Vice President of

[1] "Overexposed: The Threats to Privacy and Security on File Sharing Networks," Committee on Government Reform, 108th Congress (May 15, 2003), Report No. 108–26.

Worldwide Operations, Brilliant Digital Entertainment; and Mari J. Frank, Esq., Mari J. Frank, Esq. & Associates.

On May 15, 2003, the Committee on Government Reform released a staff report entitled "File-Sharing Programs and Peer-To-Peer Networks: Privacy and Security Risks."[2] This report summarizes the results of the Committee's staff investigation into the potential privacy and security risks associated with the use of peer-to-peer file-sharing programs. Committee staff found that many users of file-sharing programs have inadvertently made highly personal information available to other users and that file-sharing software can spread viruses, worms, and other malicious computer files.

SECTION-BY-SECTION

Section 1. Short title

The short title of this bill is the "Government Network Security Act of 2003."

Section 2. Findings

This section details the findings of Congress that peer-to-peer file sharing can pose security and privacy threats to computers and networks. Specifically, peer-to-peer file sharing can expose classified and sensitive information stored on computers or networks, act as a point of entry for viruses and other malicious programs, consume network resources, and expose identifying information about host computers that can be used by hackers to select potential targets.

This section also finds that the House of Representatives and the Senate are using methods to protect the security and privacy of congressional computers and networks from the risks posed by peer-to-peer file sharing.

This section also finds that any potentially beneficial innovations in peer-to-peer technology for government applications can be pursued on state, local, and federal networks. Use of peer-to-peer file sharing programs in this way does pose risks to network security because it does not expose government computers and networks to nongovernmental users.

Section 3. Protection of government computers from risks of peer-to-peer file sharing

This section requires that, as part of the federal agency responsibilities set forth by the Federal Information Security Act of 2002 (44 U.S.C. 3544 and 44 U.S.C. 3545), each agency develop and implement a plan to protect the security and privacy of computers and networks from the risks posed by peer-to-peer file sharing. These plans will include the use of appropriate methods for each agency to achieve this goal, including technological means such as software and hardware and non-technological means such as employee training. Each agency is required to develop and implement the plan no later than six months after enactment of this Act and review and revise the plan periodically as necessary.

This section also directs the Comptroller General to review the adequacy of agency plans and submit to the Committee on Govern-

[2] Ibid., p. 125.

ment Reform of the House of Representatives and the Committee on Governmental Affairs of the Senate a report on the results of the review no later than 18 months after enactment of this act. To facilitate evaluation, each agency should provide a copy of the plan required under this Act to the Comptroller General, preferably in electronic form. Each agency should also provide the General Accounting Office with a description of the agency's policy concerning the use of peer-to-peer applications by employees, how the agency plans to monitor employee compliance with this policy, how the agency plans to enforce the policy, how the agency plans to address peer-to-peer applications in its employee training programs, the technological tools that agencies plan to use to monitor and prevent inappropriate use of peer-to-peer applications, and a timetable for implementing the plan including any significant barriers to implementation. The requirement by the Comptroller General to review such plans shall be satisfied by reviewing a sample of the plans provided.

Section 4. Definitions

This section defines the term "peer-to-peer file sharing" to mean the use of computer software, other than computer and network operating systems, that has as its primary function the capability to allow the computer on which such software is used to designate files available for transmission to another computer using such software, to transmit files directly to another such computer, and to request the transmission of files from another such computer. The term does not include the use of such software for file sharing between, among, or within State, local, or Federal government agencies.

This section defines "agency" to have the meaning provided by section 3502 of title 44, United States Code.

EXPLANATION OF AMENDMENTS

The Committee reported the bill without amendment.

COMMITTEE CONSIDERATION

On September 25, the Committee met in open session and ordered reported favorably the bill, H.R. 3159 by voice vote.

ROLLCALL VOTES

No rollcall votes were held.

APPLICATION OF LAW TO THE LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(B)(3) of the Congressional Accountability Act (Public Law 104–1).

STATEMENT OF OVERSIGHT FINDINGS AND RECOMMENDATIONS OF THE COMMITTEE

In compliance with clause 3(c)(1) of rule XIII and clause (2)(b)(1) of rule X of the Rules of the House of Representatives, the Committee reports that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X

of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

H.R. 3159 does not authorize funding. Therefore, clause 3(c)(4) of rule XIII of the Rules of the House of Representatives is inapplicable.

CONSTITUTIONAL AUTHORITY STATEMENT

Under clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee must include a statement citing the specific powers granted to Congress to enact the law proposed by H.R. 3159. The Committee finds that clauses 1 and 18 of Article I, Section 8 of the U.S. Constitution grant Congress the power to enact this law.

UNFUNDED MANDATE STATEMENT

Section 423 of the Congressional Budget and Impoundment Control Act (as amended by Section 101(a)(2) of the Unfunded Mandate Reform Act, P.L. 104–4) requires a statement whether the provisions of the reported include unfunded mandates. In compliance with this requirement the Committee has received a letter from the Congressional Budget Office included herein.

COMMITTEE ESTIMATE

Clause 3(d)(2) of rule XIII of the Rules of the House of Representatives requires an estimate and a comparison by the Committee of the costs that would be incurred in carrying out H.R. 3159. However, clause 3(d)(3)(B) of that rule provides that this requirement does not apply when the Committee has included in its report a timely submitted cost estimate of the bill prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act.

CHANGES IN EXISTING LAW MADE BY THE BILL AS REPORTED

Clause 3(e) of rule XIII of the Rules of the House of Representatives requires a comparative statement on changes made to existing law proposed by the bill as reported. This bill proposes no changes to existing law.

BUDGET AUTHORITY AND CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the Congressional Budget Act of 1974 and with respect to requirements of clause 3(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the Congressional Budget Act of 1974, the Committee has received the following cost estimate for H.R. 3159 from the Director of Congressional Budget Office:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 6, 2003.

Hon. TOM DAVIS,
Chairman, Committee on Government Reform,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 3159, the Government Network Security Act of 2003.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Matthew Pickford.

Sincerely,

DOUGLAS HOLTZ-EAKIN,
Director.

Enclosure.

H.R. 3159—Government Network Security Act of 2003

H.R. 3159 would require federal agencies develop and implement a plan within a six months to ensure computer systems are secure from the use of Internet file-sharing (peer-to peer) programs. Peer-to-peer file-sharing programs are Internet applications that allow users to download and directly share electronic files from other users on the same network. The legislation would not prohibit the use of file-sharing programs, but would require agencies to create a plan that uses technology and employee training to address potential privacy and security concerns for government computer networks. The legislation also would require the General Accounting Office (GAO) to review individual agency plans within 18 months after enactment.

CBO estimates that implementing H.R. 3159 would not have a significiant impact on the federal budget. Under the E-Government Act of 2002, federal agencies are already charged with protecting information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. H.R. 3159 would highlight a specific security concern for computer systems that federal agencies are currently implementing plans to protect. Based on information from the Office of Management and Budget and GAO, CBO expects that addressing this specific security concern would not significantly increase the cost of ongoing efforts to maintain secure federal computer systems.

In addition, the legislation would require the GAO to review and report on the individual agencies plans. CBO expects that completing the GAO report would cost less than $500,000, assuming the availability of appropriated funds.

The bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of state, local, or tribal governments.

The CBO staff contact for this estimate is Matthew Pickford. This estimate was approved by Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

○